UNITED STATES PATENT AND TRADEMARK OFFICE

A

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/998,915	11/30/2001	Francisco J. Villavicencio	OBLX-01027US0	4254

51206   7590   09/21/2005

TOWNSEND AND TOWNSEND AND CREW LLP
TWO EMBARCADERO CENTER
8TH FLOOR
SAN FRANCISCO, CA. 94111-3834

EXAMINER
JEAN GILLES, JUDE

ART UNIT	PAPER NUMBER
2143	

DATE MAILED: 09/21/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
Office Action Summary	09/998,915	VILLAVICENCIO, FRANCISCO J.
	Examiner	Art Unit
	Jude J. Jean-Gilles	2143

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>30 November 2001</u>.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-48</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-48</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>30 November 2001</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date <u>02/28/2002</u>.

4)☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

DETAILED ACTION

This office action is responsive to communication filed on 11/30/2001.

Information Disclosure Statement

1.   The references listed on the Information Disclosure Statement submitted on

02/28/2002 have been considered by the examiner (see attached PTO-1449A).

Claim Rejections - 35 USC § 102

2.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3.   **Claims 1-48** are rejected under 35 U.S.C. 102(e) as being unpatentable by

Purpura et al (Purpura) U.S. Patent No. 6,421,768 B1.

Regarding claim 1, Purpura discloses a method for impersonating, comprising

the steps of:

receiving authentication credentials for a first entity and an identification of a

second entity (column 3, lines 27-48);

authenticating said first entity based on said authentication credentials for said

first entity (column 3, lines 16-26);

creating a cookie that stores an indication of said second entity if said step of

authenticating is performed successfully (column 3, lines 27-48); and

authorizing said first entity to access a first resource as said second entity based on

said cookie (column 3, lines 27-59).

Regarding claim 2, Purpura discloses a method according to claim 1, further

comprising the step of: providing a form for said authentication credentials, said form

includes a request for a user identification, a password and an impersonated

identification, said user identification and said password correspond to said

authentication credentials for said first entity, said impersonated identification

corresponds to said identification of said second entity (column 3, lines 37-59; note that

the voucher represents the inside the cookie).

Regarding claim 3, Purpura discloses a method according to claim 1, wherein:

said step of receiving is performed by an access system; said access system protects

said first resource; and said first resource is separate from said access system (column

3, lines 27-69).

Regarding claim 4, Purpura discloses a method according to claim 1, wherein:

said step of receiving is performed by an access system; said access system protects a

plurality of resources; and said plurality of resources includes said first resource

(column 3, lines 27-69).

Regarding claim 5, Purpura discloses a method according to claim 1, wherein:

said cookie stores a distinguished name of said second entity and an IP address for

said first entity (column 4, lines 44-67; column 5, lines 1-15).

Regarding claim 6, Purpura discloses a method accord to claim 1, further

comprising the steps of:

receiving a request to access said first resource; providing a form for said

authentication credentials, said form includes a request for a user identification, a

password and an impersonates identification, said user identification and said password

correspond to said authentication credentials for said first entity, said impersonated

identification corresponds to said identification of said second entity; and transmitting

said cookie for storage on a device being used by said first entity to send said request

to access said first resource (column 4, lines 44-67; column 5, lines 1-15).

Regarding claim 7, Purpura discloses a method according to claim 1, wherein:

said steps of receiving, authenticating and authorizing are performed by an access

system; said access system provides access management services and identity

management services; and said first resource is protected by, but separate from, said

access system (column 4, lines 44-67; column 5, lines 1-15).

Regarding claim 8, Purpura discloses a method according to claim 1, wherein:

said authentication credentials include an ID and a password; said step of

authenticating includes the steps of:

searching a directory server for a first user identity profile that matches said ID,

verifying said password based on said user identity profile (column 3, lines 27-

67),

searching said directory server for a second user identity profile that matches

said identification of said second entity(column 3, lines 27-67), and

accessing one or more attributes of said second user identity profile; and

said cookie includes said one or more attributes of said second user identity

profile (column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15).

Regarding claim 9, Purpura discloses a method according to claim 8, wherein:

said steps of searching a directory server for a first user identity profile and verifying

said password based on said user identity profile are performed by a first authentication

plug-in (column 3, lines 27-67); and

said steps of searching said directory server for a second user identity profile and

accessing one or more attributes of said second user identity profile are performed by a

second authentication plug-in (column 4, lines 44-67; column 5, lines 1-15).

Regarding claim 10, Purpura discloses a method according to claim 1, wherein:

said cookie stores a distinguished name for said second entity; and said step of

authorizing includes the steps of: accessing said distinguished name stored in said

cookie, accessing a user identity profile for said second entity based on said

distinguished name, accessing a set of one or more authorization rules for said first

resource, and comparing attributes of said user identity profile for said second entity to

said set of one or more authorization rules for said first resource (column 3, lines 27-67;

column 4, lines 44-67; column 5, lines 1-15).

Regarding claim 11, Purpura discloses a method according to claim 1, wherein:

said authentication credentials correspond to a set of attributes for said first entity; said

identification of said second entity corresponds to a set of attributes for said second

entity; said step of authorizing is based on one or more of said attributes for said first

entity; and said step of authorizing is based on one or more of said attributes for said

second entity (column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15).

Regarding claim 12, Purpura discloses a method according to claim 1, wherein:

said authentication credentials correspond to a set of attributes for said first entity; and

said step of authorizing is not based on attributes for said first entity (column 3, lines 27-

67; column 4, lines 44-67; column 5, lines 1-15).

Regarding claim 13, Purpura discloses a method according to claim 1, further

comprising the steps of: receiving a request for a login form; and providing said login

form, said login form includes a request for a user identification, a password and an

impersonated identification, said user identification and said password correspond to

said authentication credentials for said first entity, said impersonated identification

corresponds to said identification of said second entity. includes said first resource

(column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15).

Regarding claim 14, Purpura discloses a method according to claim 1, further

comprising the steps of: receiving a request from said first entity to access a second

resource after said step of creating said cookie; accessing contents of said cookie and

determining not to authenticate said first entity in response to said request to access

said second resource; and authorizing said first entity to access said second resource

as said second entity based on said cookie, said step of authorizing said first entity to

access said second resource is performed without authenticating said first entity in

response to said request to access said second resource. includes said first resource

(column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15).

Regarding claim 15, Purpura discloses a method according to claim 1, wherein:

said steps of authenticating and authorizing are performed without knowing a password

for said second entity. includes said first resource (column 3, lines 27-67; column 4,

lines 44-67; column 5, lines 1-15).

Regarding claim 16, Purpura discloses a method for impersonating, comprising

the steps of:

receiving authentication credentials for a first entity and an identification of a

second entity at an access system, said access system protects a first resource that is

separate from said access system column 3, lines 27-67; column 4, lines 44-67; column

5, lines 1-15);

authenticating said first entity based on said authentication credentials for said

first entity, said step of authenticating is performed by said access system (column 3,

lines 27-67; column 4, lines 44-67; column 5, lines 1-15); and

authorizing said first entity to access said first resource as said second entity,

said step of authorizing is performed by said access system. includes said first resource

(column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15).).

Regarding claim 17, Purpura discloses a method according to claim 16,

wherein:

said steps of authenticating and authorizing are performed without knowing a

password for said second entity (column 3, lines 27-67; column 4, lines 44-67; column

5, lines 1-15).

Regarding claim 18, Purpura discloses a method according to claim 16,

wherein:

said access system protects a plurality of resources that are separate from said

access system; and said plurality of resources includes said first resource (column 3,

lines 27-67; column 4, lines 44-67; column 5, lines 1-15).

Regarding claim 19, Purpura discloses a method according to claim 16,

wherein:

said authentication credentials include an ID and a password (column 3, lines 27-

67; column 4, lines 44-67; column 5, lines 1-15);

said step of authenticating includes the steps of:

searching a directory server for a first user identity profile that matches

said ID,

verifying said password based on said user identity profile (column 3, lines

27-67; column 4, lines 44-67; column 5, lines 1-15),

searching said directory server for a second user identity profile that

matches said identification of said second entity(column 3, lines 27-67; column 4, lines

44-67; column 5, lines 1-15), and

accessing one or more attributes of said second user identity profile; and

said step of authorizing uses said one or more attributes of said second user identity

profile (column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15).

Regarding claim 20, Purpura discloses a method according to claim 16,

wherein:

said steps of searching a directory server for a first user identity profile and

verifying said password based on said user identity profile are performed by a first

authentication plug-in (column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-

15); and

said steps of searching said directory server for a second user identity profile and

accessing one or more attributes of said second user identity profile are performed by a

second authentication plug-in (column 4, lines 44-67; column 5, lines 1-15).

Regarding claim 21, Purpura discloses a method according to claim 16,

wherein:

said step of authenticating provides a name for said second entity (column 3,

lines 27-67; column 4, lines 44-67; column 5, lines 1-15), and

said step of authorizing includes the steps of: accessing said name,

accessing a user identity profile for said second entity based on said

name, accessing a set of one or more authorization rules for said resource, and

comparing attributes of said user identity profile for said second entity to said set of one

or more authorization rules for said resource (column 3, lines 27-67; column 4, lines 44-

67; column 5, lines 1-15).

Regarding claim 22, Purpura discloses a method according to claim 16,

wherein:

said authentication credentials correspond to a set of attributes for said first

entity; said identification of said second entity corresponds to a set of attributes for said

second entity; said step of authorizing is based on one or more of said attributes for said

first entity; and said step of authorizing is based on one or more of said attributes for

said second entity (column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15).

Regarding claim 23, Purpura discloses a method according to claim 16, further

comprising the steps of:

receiving a request to access a second resource from said first entity after said

step of authenticating said first entity, said access system protects said second

resource; and authorizing said first entity to access said second resource as said

second entity, said step of authorizing said first entity to access said second resource is

performed without authenticating said first entity in response to said request to access

said second resource (column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-

15).

Regarding claim 24, Purpura discloses a method for impersonating, comprising

the steps of:

receiving authentication credentials for a first entity and an identification of a

second entity at an access system, said access system protects a plurality of resources;

receiving an indication of one or more of said plurality of resources(column 3,

lines 27-67; column 4, lines 44-67; column 5, lines 1-15);

authenticating said first entity based on said authentication credentials for said

first entity, said step of authenticating is performed by said access system (column 3,

lines 27-67; column 4, lines 44-67; column 5, lines 1-15); and

authorizing said first entity to access said one or more of said plurality of

resources as said second user, said step of authorizing is performed by said access

system(column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15).

Regarding claim 25, Purpura discloses a method according to claim 24,

wherein:

said authentication credentials include an ID and a password (column 3, lines 27-

67; column 4, lines 44-67; column 5, lines 1-15);

said step of authenticating includes the steps of:

searching a directory server for a first user identity profile that matches

said ID (column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15)'

verifying said password based on said user identity profile, searching said

directory server for a second user identity profile that matches said identification of said

second entity, and accessing one or more attributes of said second user identity profile;

and said step of authorizing uses said one or more attributes of said second user

identity profile (column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15).

Regarding claim 26, Purpura discloses a method according to claim 24,

wherein: said step of authenticating provides a name for said second entity; and said

step of authorizing includes the steps of: accessing said name, accessing a user identity

profile for said second entity based on said name, accessing a set of one or more

authorization rules for said resource, and comparing attributes of said user identity

profile for said second entity to said set of one or more authorization rules (column 3,

lines 27-67; column 4, lines 44-67; column 5, lines 1-15).

Regarding claim 27, Purpura discloses a method according to claim 24, wherein: said authentication credentials correspond to a set of attributes for said first entity; said identification of said second entity corresponds to a set of attributes for said second entity; said step of authorizing is based on one or more attributes for said first entity; and said step of authorizing is not based on attributes for said first entity (column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15).

Regarding claim 28, Purpura discloses one or more processor readable storage devices having processor readable code embodied on said processor readable storage devices, said processor readable code for programming one or more processors to perform a method comprising the steps of:

receiving authentication credentials for a first entity and an identification of a second entity (column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15); authenticating said first entity based on said authentication credentials for said first entity; creating a cookie that stores an indication of said second entity if said step of authenticating is performed successfully (column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15); and

authorizing said first entity to access a first resource as said second entity based on said cookie (column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15).

Regarding claim 29, Purpura discloses one or more processor readable storage devices according to claim 28, wherein: said steps of receiving, authenticating and authorizing are performed by an access system; said access system protects a plurality

of resources separate from said access system; and said plurality of resources includes

said first resource (column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15).

Regarding claim 30, Purpura discloses one or more processor readable storage

devices according to claim 28, wherein: said cookie stores a distinguished name of said

second entity and an IP address for said first entity (column 3, lines 27-67; column 4,

lines 44-67; column 5, lines 1-15).

Regarding claim 31, Purpura discloses one or more processor readable storage

devices according to claim 28, wherein: said authentication credentials include an ID

and a password; said step of authenticating includes the steps of: searching a directory

server for a first user identity profile that matches said ID, verifying said password based

on said user identity profile, searching said directory server for a second user identity

profile that matches said identification of said second entity, and accessing one or more

attributes of said second user identity profile; and said cookie includes said one or more

attributes of said second user identity profile (column 3, lines 27-67; column 4, lines 44-

67; column 5, lines 1-15).

Regarding claim 32, Purpura discloses one or more processor readable storage

devices according to claim 28, wherein: said cookie stores a distinguished name for

said second entity; and said step of authorizing includes the steps of: accessing said

distinguished name stored in said cookie, accessing a user identity profile for said

second entity based on said distinguished name, accessing a set of one or more

authorization rules for said first resource, and comparing attributes of said user identity

profile for said second entity to said set of one or more authorization rules for said first

resource (column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15).

Regarding claim 33, Purpura discloses one or more processor readable storage

devices according to claim 28, wherein: said authentication credentials correspond to a

set of attributes for said first entity; said identification of said second entity corresponds

to a set of attributes for said second entity; said step of authorizing is based on one or

more of said attributes for said first entity; and said step of authorizing is based on one

or more of said attributes for said second entity (column 3, lines 27-67; column 4, lines

44-67; column 5, lines 1-15).

Regarding claim 34, Purpura discloses one or more processor readable storage

devices according to claim 28, wherein: receiving a request from said first entity to

access a second resource after said step of creating said cookie; accessing contents of

said cookie and determining not to authenticate said first entity in response to said

request to access said second resource; and authorizing said first entity to access said

second resource as said second entity based on said cookie, said step of authorizing

said first entity to access said second resource is performed without authenticating said

first entity in response to said request to access said second resource (column 3, lines

27-67; column 4, lines 44-67; column 5, lines 1-15).

Regarding claim 35, Purpura discloses an apparatus for providing access

management that allows for impersonating, comprising:

    a communication interface (column 5, lines 16-33);

    a storage device (fig. 1, items 100, 110, and 120); and

a processing unit in communication with said communication interface and said

storage device, said processing unit performs a method comprising the steps of:

receiving authentication credentials for a first entity and an identification of

a second entity (column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15),

authenticating said first entity based on said authentication credentials for

said first entity (column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15),

creating a cookie that stores an indication of said second entity if said step

of authenticating is performed successfully, and authorizing said first entity to access a

first resource as said second entity based on said cookie (column 3, lines 27-67; column

4, lines 44-67; column 5, lines 1-15).

Regarding claim 36, Purpura discloses an apparatus according to claim 35,

wherein: said steps of receiving, authenticating and authorizing are performed by an

access system; said access system protects a plurality of resources separate from said

access system; and said plurality of resources includes said first resource (column 3,

lines 27-67; column 4, lines 44-67; column 5, lines 1-15).

Regarding claim 37, Purpura discloses an apparatus according to claim 35,

wherein: said authentication credentials include an ID and a password; said step of

authenticating includes the steps of: searching a directory server for a first user identity

profile that matches said ID, verifying said password based on said user identity profile,

searching said directory server for a second user identity profile that matches said

identification of said second entity, and accessing one or more attributes of said second

user identity profile; and said cookie includes said one or more attributes of said second

user identity profile (column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15).

Regarding claim 38, Purpura discloses an apparatus according to claim 35,

wherein: said cookie stores a distinguished name for said second entity; and said step

of authorizing includes the steps of: accessing said distinguished name stored in said

cookie, accessing a user identity profile for said second entity based on said

distinguished name, accessing a set of one or more authorization rules for said first

resource, and comparing attributes of said user identity profile for said second entity to

said set of one or more authorization rules for said first resource.

Regarding claim 39, Purpura discloses one or more processor readable storage

devices having processor readable code embodied on said processor readable storage

devices, said processor readable code for programming one or more processors to

perform a method comprising the steps of:

receiving authentication credentials for a first entity and an identification of a

second entity at an access system, said access system protects a first resource that is

separate from said access system (column 3, lines 27-67; column 4, lines 44-67;

column 5, lines 1-15).

authenticating said first entity based on said authentication credentials for said

first entity, said step of authenticating is performed by said access system (column 3,

lines 27-67; column 4, lines 44-67; column 5, lines 1-15); and

authorizing said first entity to access said first resource as said second entity,

said step of authorizing is performed by said access system (column 3, lines 27-67;

column 4, lines 44-67; column 5, lines 1-15).

Regarding claim 40, Purpura discloses one or more processor readable storage

devices according to claim 39, wherein: said access system protects a plurality of

resources that are separate from said access system; and said plurality of resources

includes said first resource (column 3, lines 27-67; column 4, lines 44-67; column 5,

lines 1-15).

Regarding claim 41, Purpura discloses one or more processor readable storage

devices according to claim 39, wherein: said authentication credentials include an ID

and a password; said step of authenticating includes the steps of: searching a directory

server for a first user identity profile that matches said ID, verifying said password based

on said user identity profile, searching said directory server for a second user identity

profile that matches said identification of said second entity, and accessing one or more

attributes of said second user identity profile; and said step of authorizing uses said one

or more attributes of said second user identity profile (column 3, lines 27-67; column 4,

lines 44-67; column 5, lines 1-67).

Regarding claim 42, Purpura discloses one or more processor readable storage

devices according to claim 39, wherein: said step of authenticating provides a name for

said second entity; and said step of authorizing includes the steps of: accessing said

name, accessing a user identity profile for said second entity based on said name,

accessing a set of one or more authorization rules for said resource, and comparing

attributes of said user identity profile for said second entity to said set of one or more

authorization rules for said resource (column 3, lines 27-67; column 4, lines 44-67;

column 5, lines 1-67).

Regarding claim 43, Purpura discloses one or more processor readable storage

devices according to claim 39, wherein: said authentication credentials correspond to a

set of attributes for said first entity; said identification of said second entity corresponds

to a set of attributes for said second entity; said step of authorizing is based on one or

more of said attributes for said first entity; and said step of authorizing is based on one

or more of said attributes for said second entity (column 3, lines 27-67; column 4, lines

44-67; column 5, lines 1-67).

Regarding claim 44, Purpura discloses one or more processor readable storage

devices according to claim 39, wherein said method further comprises the steps of:

receiving a request to access a second resource from said first entity after said step of

authenticating said first entity, said access system protects said second resource; and

authorizing said first entity to access said second resource as said second entity, said

step of authorizing said first entity to access said second resource is performed without

authenticating said first entity in response to said request to access said second

resource (column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-67).

Regarding claim 30, Purpura discloses an apparatus for providing access

management that allows for impersonating, comprising:

a communication interface (column 5, lines 16-33);

a storage device (fig. 1, items 100, 110, and 120); and

a processing unit in communication with said communication interface and said

storage device, said processing unit performs a method comprising the steps of:

receiving authentication credentials for a first entity and an identification of

a second entity at an access system, said access system protects a first resource that is

separate from said access system (column 3, lines 27-67; column 4, lines 44-67;

column 5, lines 1-15),

authenticating said first entity based on said authentication credentials for

said first entity, said step of authenticating is performed by said access system (column

3, lines 27-67; column 4, lines 44-67; column 5, lines 1-15), and

authorizing said first entity to access said first resource as said second entity,

said step of authorizing is performed by said access system (column 3, lines 27-67;

column 4, lines 44-67; column 5, lines 1-15).

Regarding claim 46, Purpura discloses an apparatus according to claim 45,

wherein: said access system protects a plurality of resources that are separate from

said access system; and said plurality of resources includes said first resource.

Regarding claim 47, Purpura discloses an apparatus according to claim 45,

wherein: said authentication credentials include an ID and a password; said step of

authenticating includes the steps of: searching a directory server for a first user identity

profile that matches said ID, verifying said password based on said user identity profile,

searching said directory server for a second user identity profile that matches said

identification of said second entity, and accessing one or more attributes of said second

user identity profile; and said step of authorizing uses said one or more attributes of said

second user identity profile (column 3, lines 27-67; column 4, lines 44-67; column 5,

lines 1-67).

Regarding claim 48, Purpura discloses an apparatus according to claim 45,

wherein: said step of authenticating provides a name for said second entity; and said

step of authorizing includes the steps of: accessing said name, accessing a user identity

profile for said second entity based on said name, accessing a set of one or more

authorization rules for said resource, and comparing attributes of said user identity

profile for said second entity to said set of one or more authorization rules for said

resource (column 3, lines 27-67; column 4, lines 44-67; column 5, lines 1-67).

Conclusion

4. Any inquiry concerning this communication or earlier communications from examiner

should be directed to Jude Jean-Gilles whose telephone number is (571) 272-3914.

The examiner can normally be reached on Monday-Thursday and every other Friday

from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, David Wiley, can be reached on (571) 272-3923. The fax phone number for

the organization where this application or proceeding is assigned is (703) 305-3719.

Any inquiry of a general nature or relating to the status of this application or

proceeding should be directed to the receptionist whose telephone number is (703) 305-

3900.

Jude Jean-Gilles

Patent Examiner

Art Unit 2143

DAVID WILEY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

JJG

September 15, 2005